(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **2000196582 A**

(43) Date of publication of application: **14 . 07 . 00**

(51) Int. Cl **H04L 9/08**
G06F 12/14
G09C 1/00

(21) Application number: **10371529**

(22) Date of filing: **25 . 12 . 98**

(71) Applicant: **NIPPON TELEGR & TELEPH CORP <NTT>**

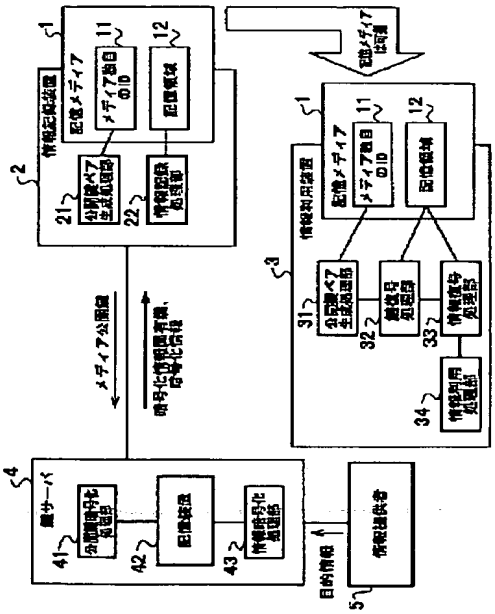
(72) Inventor: **UENO MASAMI**
SONEOKA AKINAO
MIYAKE NOBUHISA
IORI SACHIKO
ARITA KAZUO

(54) **METHOD FOR RECORDING, UTILIZING AND INFORMATION FOR PREVENTING ILLEGAL USE BY EMPLOYING STORAGE MEDIA IDENTIFIER**

(57) Abstract:

PROBLEM TO BE SOLVED: To provide a method for recording, utilizing and delivering information for preventing illegal use by employing a storage medium identifier where the identifier unique to the storage media is used and the identifier cannot be used even when it is copied to other storage media.

SOLUTION: A key server 4 uses an information specific key to encrypt object information, a storage device 42 stores encrypted information and the information specific key, an information recorder 2 uses an ID 11 unique to a storage media 1 to generate a medium public key and a media secret key and delivers the media public key to the server 4. The server 4 delivers an encrypted information specific key resulting from encrypting the information specific key with the media public key and the encryption information to the information recorder 2, which records the encrypted information specific key and the encrypted information to the storage media 1. An information utilizing device 3 decodes the encrypted information by using the information specific key obtained by decording the encrypted information specific key with the medium private key generated from the ID 11 unique to the media and extracts object information.



PATENT ABSTRACTS OF JAPAN

(11) Publication number : 2000-196582

(43) Date of publication of application : 14.07.2000

(51) Int. Cl. H04L 9/08
G06F 12/14
G09C 1/00

(21) Application number : 10-371529

(22) Date of filing : 25.12.1998

(71) Applicant : NIPPON TELEGR & TELEPH CORP <NTT>

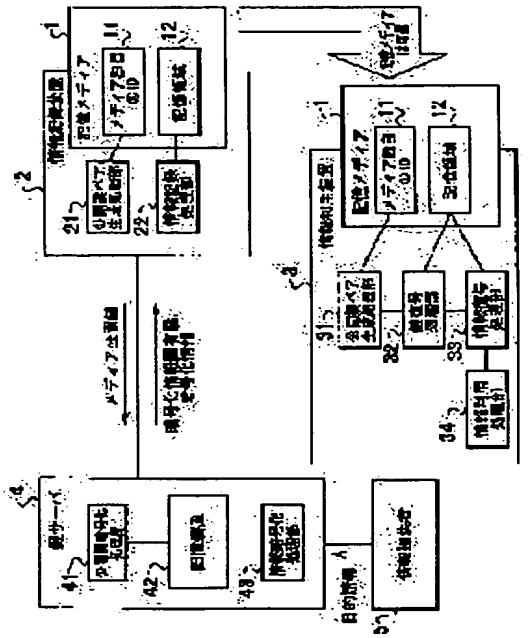
(72) Inventor : UENO MASAMI
SONEOKA AKINAO
MIYAKE NOBUHISA
IORI SACHIKO
ARITA KAZUO

(54) METHOD FOR RECORDING, UTILIZING AND INFORMATION FOR PREVENTING ILLEGAL USE BY EMPLOYING STORAGE MEDIA IDENTIFIER

(57) Abstract:

PROBLEM TO BE SOLVED: To provide a method for recording, utilizing and delivering information for preventing illegal use by employing a storage medium identifier where the identifier unique to the storage media is used and the identifier cannot be used even when it is copied to other storage media.

SOLUTION: A key server 4 uses an information specific key to encrypt object information, a storage device 42 stores encrypted information and the information specific key, an information recorder 2 uses an ID 11 unique to a storage media 1 to generate a medium public key and a media secret key and delivers the media public key to the server 4. The server 4 delivers an encrypted information specific key resulting from encrypting the information specific key with the media public key and the encryption information to the information recorder 2, which records the encrypted information specific key and the encrypted information to the storage media 1. An information utilizing device 3 decodes the encrypted information by using the information specific key obtained by decording the encrypted information specific key with the medium private key generated from the ID 11 unique to the media and extracts object information.



LEGAL STATUS

[Date of request for examination] 17.04.2001
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号
特開2000－196582
（Ｐ２０００－１９６５８２Ａ）
(43)公開日　平成12年７月14日(2000.7.14)

(51)Int.Cl.⁷	識別記号	ＦＩ			テーマコード（参考）
H04L 9/08		H04L 9/00	601	B	5B017
G06F 12/14	320	G06F 12/14	320	B	5J104
G09C 1/00	620	G09C 1/00	620	Z	9A001
	630		630	B	
	660		660	A	

審査請求　未請求　請求項の数12　ＯＬ　（全15頁）

(21)出願番号　特願平10－371529

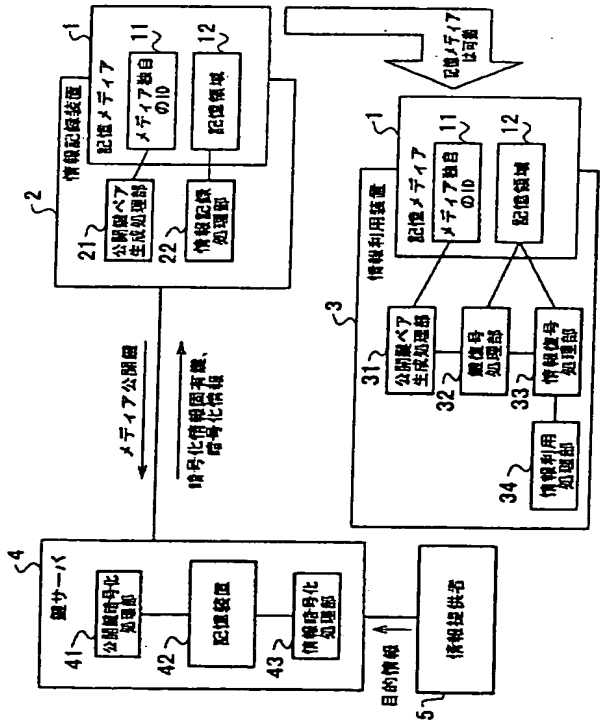
(22)出願日　平成10年12月25日(1998.12.25)

(71)出願人　000004226
日本電信電話株式会社
東京都千代田区大手町二丁目３番１号
(72)発明者　上野　正巳
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内
(72)発明者　曽根岡　昭直
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内
(74)代理人　100083806
弁理士　三好　秀和　（外１名）

最終頁に続く

(54)【発明の名称】記憶メディア識別子を利用した不正利用防止のための情報記録、利用および配送方法

(57)【要約】
【課題】　記憶メディア独自の識別子を利用し、他の記憶メディアに複製しても利用できないようにした記憶メディア識別子を利用した不正利用防止のための情報記録、利用および配送方法を提供する。
【解決手段】　鍵サーバ４で情報固有鍵で目的情報を暗号化し、暗号化情報と情報固有鍵を記憶装置４２に記憶し、情報記録装置２で記憶メディア１独自のＩＤ１１を用いてメディア公開鍵とメディア秘密鍵を生成し、メディア公開鍵をサーバ４に配送し、サーバ４はメディア公開鍵で情報固有鍵を暗号化した暗号化情報固有鍵と暗号化情報を情報記録装置２に配送し、暗号化情報固有鍵と暗号化情報を記憶メディア１に記録し、情報利用装置３ではメディア独自のＩＤ１１から生成したメディア秘密鍵で暗号化情報固有鍵を復号して取り出した情報固有鍵で暗号化情報を復号して目的情報を取り出す。



1

【特許請求の範囲】

【請求項１】　書換え不可能な独自の識別子を有する記憶メディアを用いて情報の記録を行う情報記録方法であって、

前記記憶メディアの識別子を利用して、公開鍵方式のメディア公開鍵とメディア秘密鍵を生成し、

不正利用を防止したい目的情報に対して情報固有鍵を生成し、この情報固有鍵を用いて前記目的情報を暗号化した暗号化情報を生成し、

前記情報固有鍵を前記メディア公開鍵で暗号化した暗号化情報固有鍵を生成し、

前記暗号化情報と前記暗号化情報固有鍵を記憶メディアに記録することを特徴とする記憶メディア識別子を利用した不正利用防止のための情報記録方法。

【請求項２】　書換え不可能な独自の識別子を有する記憶メディアに記録された情報の利用を行う情報利用方法であって、

前記記憶メディアの識別子を利用して、公開鍵方式のメディア公開鍵とメディア秘密鍵を生成し、

不正利用を防止したい目的情報に対して生成された情報固有鍵を用いて目的情報を暗号化した暗号化情報と前記情報固有鍵を前記メディア公開鍵で暗号化した暗号化情報固有鍵を記録している前記記憶メディアから前記暗号化情報固有鍵を読み出し、

この読み出した暗号化情報固有鍵を前記メディア秘密鍵で復号して、情報固有鍵を取り出し、

前記暗号化情報を前記記憶メディアから読み出し、この暗号化情報を前記情報固有鍵で復号して前記目的情報を取り出して利用することを特徴とする記憶メディア識別子を利用した不正利用防止のための情報利用方法。

【請求項３】　サーバにおいて不正利用を防止したい目的情報に対して生成された情報固有鍵を用いて目的情報を暗号化した暗号化情報と情報固有鍵をサーバ記憶装置に蓄積し、この蓄積されている暗号化情報と情報固有鍵を、情報記録装置に装着され、書換え不可能な独自の識別子を有する記憶メディアまで配送する情報配送方法であって、

前記記憶メディアの識別子を利用して、公開鍵方式のメディア公開鍵とメディア秘密鍵を生成し、このメディア公開鍵をサーバに送信し、

サーバにおいて前記メディア公開鍵で前記情報固有鍵を暗号化して暗号化情報固有鍵を生成し、

前記暗号化情報固有鍵と前記暗号化情報を情報記録装置に送信し、

情報記録装置は前記暗号化情報固有鍵と前記暗号化情報を受信して、記憶メディアに記録することを特徴とする記憶メディア識別子を利用した不正利用防止のための情報配送方法。

【請求項４】　情報提供側からの目的情報を情報利用側に配送し、書換え不可能な独自の識別子を有する記憶メディアに目的情報を記録し、この記録された目的情報を利用する情報の配送、記録および利用方法であって、

情報提供側において、前記目的情報に対して情報固有鍵を生成し、この生成した情報固有鍵を用いて前記目的情報を暗号化した暗号化情報を生成し、この暗号化情報と前記情報固有鍵を記憶しておき、

情報利用側において、前記記憶メディアの識別子を利用して、公開鍵方式のメディア公開鍵とメディア秘密鍵を生成し、このメディア公開鍵を情報提供側に配送し、

情報提供側において、前記メディア公開鍵を受信し、このメディア公開鍵で前記情報固有鍵を暗号化した暗号化情報固有鍵を生成し、この生成した暗号化情報固有鍵と前記暗号化情報を情報利用側に配送し、

情報利用側において、前記暗号化情報固有鍵と前記暗号化情報を受信し、この受信した暗号化情報固有鍵と暗号化情報を前記記憶メディアに記録し、

情報利用側において、前記記憶メディアの識別子を利用して、公開鍵方式のメディア公開鍵とメディア秘密鍵を生成し、このメディア秘密鍵を用いて前記暗号化情報固有鍵を復号して情報固有鍵を取り出し、この情報固有鍵を用いて前記暗号化情報を復号して目的情報を取り出すことを特徴とする記憶メディア識別子を利用した不正利用防止のための情報配送、記録および利用方法。

【請求項５】　サーバにおいて不正利用を防止したい目的情報に対して生成された情報固有鍵を用いて目的情報を暗号化した暗号化情報が既に情報記録装置の記憶メディア内に記憶されており、サーバの記憶装置に蓄積されている情報固有鍵を、情報記録装置に装着され、書換え不可能な独自の識別子を有する記憶メディアまで配送する情報配送方法であって、

前記記憶メディアの識別子を利用して、公開鍵方式のメディア公開鍵とメディア秘密鍵を生成し、このメディア公開鍵をサーバに送信し、

サーバにおいて前記メディア公開鍵で前記情報固有鍵を暗号化して暗号化情報固有鍵を生成し、

前記暗号化情報固有鍵を情報記録装置に送信し、

情報記録装置は前記暗号化情報固有鍵を受信して、記憶メディアに記録することを特徴とする記憶メディア識別子を利用した不正利用防止のための情報配送方法。

【請求項６】　書換え不可能な独自の識別子を有する記憶メディアを用いて情報の記録を行う情報記録方法であって、

情報記録装置と情報利用装置の間で共有され、利用者には秘密の利用共通鍵を用いて、前記記憶メディアの識別子を暗号化して第１の暗号情報Ｋ１を生成し、

鍵サーバと情報記録装置の間で共有され、利用者には秘密の配送用共通鍵を用いて、前記第１の暗号情報Ｋ１を暗号化して第２の暗号情報Ｋ２を生成し、

不正利用を防止したい目的情報に対して情報固有鍵を生成し、この情報固有鍵を用いて前記目的情報を暗号化し

た暗号化情報を生成し、
前記情報固有鍵を前記第１の暗号情報Ｋ１で暗号化してＫ１暗号化情報固有鍵を生成し、
前記暗号化情報と前記Ｋ１暗号化情報固有鍵を記憶メディアに記録することを特徴とする記憶メディア識別子を利用した不正利用防止のための情報記録方法。
【請求項７】　書換え不可能な独自の識別子を有する記憶メディアに記録された情報の利用を行う情報利用方法であって、
情報記録装置と情報利用装置の間で共有され、利用者には秘密の利用共通鍵を用いて、前記記憶メディアの識別子を暗号化して第１の暗号情報Ｋ１を生成し、
前記情報固有鍵を前記第１の暗号情報Ｋ１で暗号化してＫ１暗号化情報固有鍵を生成し、
不正利用を防止したい目的情報に対して生成された情報固有鍵を用いて目的情報を暗号化した暗号化情報と前記情報固有鍵を前記第１の暗号情報Ｋ１で暗号化したＫ１暗号化情報固有鍵が記録されている記憶メディアから前記Ｋ１暗号化情報固有鍵を読み出し、
この読み出したＫ１暗号化情報固有鍵を前記第１の暗号情報Ｋ１で復号して、情報固有鍵を取り出し、
前記暗号化情報を前記記憶メディアから読み出し、この暗号化情報を前記情報固有鍵で復号して前記目的情報を取り出して利用することを特徴とする記憶メディア識別子を利用した不正利用防止のための情報利用方法。
【請求項８】　サーバにおいて不正利用を防止したい目的情報に対して生成された情報固有鍵を用いて目的情報を暗号化した暗号化情報と情報固有鍵をサーバ記憶装置に蓄積し、この蓄積されている暗号化情報と情報固有鍵を、情報記録装置に装着され、書換え不可能な独自の識別子を有する記憶メディアまで配送する情報配送方法であって、
情報記録装置と情報利用装置の間で共有され、利用者には秘密の利用共通鍵を用いて、前記記憶メディアの識別子を暗号化して第１の暗号情報Ｋ１を生成し、
サーバと情報記録装置の間で共有され、利用者には秘密の配送用共通鍵を用いて、前記第１の暗号情報Ｋ１を暗号化して第２の暗号情報Ｋ２を生成し、この第２の暗号情報Ｋ２をサーバに送信し、
サーバにおいて前記第２の暗号情報Ｋ２を前記配送用共通鍵で復号して前記第１の暗号情報Ｋ１を生成し、
この第１の暗号情報Ｋ１で前記情報固有鍵を暗号化してＫ１暗号化情報固有鍵を生成し、
前記Ｋ１暗号化情報固有鍵と前記暗号化情報を情報記録装置に送信し、
情報記録装置は前記Ｋ１暗号化情報固有鍵と前記暗号化情報を受信して、記憶メディアに記録することを特徴とする記憶メディア識別子を利用した不正利用防止のための情報配送方法。
【請求項９】　サーバにおいて不正利用を防止したい目的情報に対して生成された情報固有鍵を用いて目的情報を暗号化した暗号化情報が既に情報記録装置の記憶メディア内に記憶されており、サーバの記憶装置に蓄積されている情報固有鍵を、情報記録装置に装着され、書換え不可能な独自の識別子を有する記憶メディアまで配送する情報配送方法であって、
前記記憶メディアの識別子を利用して、公開鍵方式のメディア公開鍵とメディア秘密鍵を生成し、このメディア公開鍵をサーバに送信し、
情報記録装置と情報利用装置の間で共有され、利用者には秘密の利用共通鍵を用いて、前記記憶メディアの識別子を暗号化して第１の暗号情報Ｋ１を生成し、
サーバと情報記録装置の間で共有され、利用者には秘密の配送用共通鍵を用いて、前記第１の暗号情報Ｋ１を暗号化して第２の暗号情報Ｋ２を生成し、この第２の暗号情報Ｋ２をサーバに送信し、
サーバにおいて前記第２の暗号情報Ｋ２を前記配送用共通鍵で復号して前記第１の暗号情報Ｋ１を生成し、
この第１の暗号情報Ｋ１で前記情報固有鍵を暗号化してＫ１暗号化情報固有鍵を生成し、
前記Ｋ１暗号化情報固有鍵を情報記録装置に送信し、
情報記録装置は前記Ｋ１暗号化情報固有鍵を受信して、記憶メディアに記録することを特徴とする記憶メディア識別子を利用した不正利用防止のための情報配送方法。
【請求項１０】　書換え不可能な独自の識別子を有する記憶メディアを用いて情報の記録を行う情報記録方法であって、
前記記憶メディアの識別子を利用して、公開鍵方式のメディア公開鍵とメディア秘密鍵を生成し、
このメディア公開鍵を用いて暗号化した目的情報を記憶メディアに記録することを特徴とする記憶メディア識別子を利用した不正利用防止のための情報記録方法。
【請求項１１】　書換え不可能な独自の識別子を有する記憶メディアに記録されている暗号化情報を利用する情報利用方法であって、
前記記憶メディアの識別子を利用して、公開鍵方式のメディア公開鍵とメディア秘密鍵を生成し、
前記記憶メディアに記録されている暗号化情報を読み出し、この暗号化情報を前記メディア秘密鍵で復号して、目的情報を取り出して利用することを特徴とする記憶メディア識別子を利用した不正利用防止のための情報利用方法。
【請求項１２】　サーバに蓄積されている目的情報を、情報記録装置に装着され、書換え不可能な独自の識別子を有する記憶メディアまで配送する情報配送方法であって、
前記記憶メディアの識別子を利用して、公開鍵方式のメディア公開鍵とメディア秘密鍵を生成し、このメディア公開鍵をサーバに送信し、
サーバにおいて前記メディア公開鍵で前記目的情報を暗

5

号化して暗号化情報を生成し、
サーバは前記暗号化情報を情報記録装置に送信し、
情報記録装置は前記暗号化情報を受信して、記憶メディアに記録することを特徴とする記憶メディア識別子を利用した不正利用防止のための情報配送方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、不正利用を防止したい電子情報である目的情報を暗号化して情報提供側からの情報記録利用側に配送し、この配送された目的情報を書換え不可能な独自の識別子（以下、ＩＤと略称する）を有する記憶メディアに記録し、この記録された目的情報を利用する記憶メディア識別子を利用した不正利用防止のための情報記録、利用および配送方法に関する。

【０００２】

【従来の技術】電子情報は容易に複製可能であるという性質を持っている。一方、情報の提供者は情報に付加価値を付け、情報を販売したい場合がある。このように情報を販売する場合、情報の利用者によって情報が他のメディアに複製され、対価を払って情報を購入した正規の利用者以外に情報が利用されてしまうことがある。

【０００３】盗聴や不正利用を避けるために、情報を暗号化して配送および保存する方法が容易に考えられるが、情報を利用する際に情報を復号化するための復号鍵が必要になる。しかし、この方法では、暗号化した情報と復号鍵の両情報を複製された場合に、容易に不正利用が可能である。

【０００４】更に、これを避けるために、復号鍵を複製できない装置内に保存する場合、情報を利用するためには、復号鍵を保存した装置が必要になり、可搬性が悪くなるという問題がある。

【０００５】また、情報を販売する場合、利用者が対価を払って情報を購入する際に、情報は提供者から利用者の装置へ配送される。この配送の途中において盗聴をされた場合、盗聴した情報から元の情報が容易に再現され、対価を払って情報を購入していない盗聴者に情報が利用されてしまうことがある。

【０００６】

【発明が解決しようとする課題】上述したように、情報の提供者が販売した情報は、不正に複製された場合に、容易に不正利用されてしまうという問題がある。また、暗号化して情報を配布したとしても、暗号化した情報と、暗号化した情報を復号するための復号鍵を共に複製された場合、これも容易に不正利用されてしまうという問題がある。

【０００７】また、復号鍵の複製を避けるために、復号鍵を複製できない装置内に保存する場合、情報の可搬性が下がるという問題がある。

【０００８】更に、情報を販売する際の配送経路においても、情報が盗聴された場合に不正利用されてしまうという問題がある。

6

【０００９】本発明は、上記に鑑みてなされたもので、その目的とするところは、記憶メディア独自の書換え不可能な識別子を利用することにより他の記憶メディアに複製しても利用できないようにした記憶メディア識別子を利用した不正利用防止のための情報記録、利用および配送方法を提供することにある。

【００１０】

【課題を解決するための手段】上記目的を達成するため、請求項１記載の本発明は、書換え不可能な独自の識別子を有する記憶メディアを用いて情報の記録を行う情報記録方法であって、前記記憶メディアの識別子を利用して、公開鍵方式のメディア公開鍵とメディア秘密鍵を生成し、不正利用を防止したい目的情報に対して情報固有鍵を生成し、この情報固有鍵を用いて前記目的情報を暗号化した暗号化情報を生成し、前記情報固有鍵を前記メディア公開鍵で暗号化した暗号化情報固有鍵を生成し、前記暗号化情報と前記暗号化情報固有鍵を記憶メディアに記録することを要旨とする。

【００１１】請求項１記載の本発明にあっては、暗号化情報固有鍵から情報固有鍵を復号するにはメディア秘密鍵が必要であるが、このメディア秘密鍵は記憶メディア独自の識別子から生成されるため、記憶メディアに記録されている暗号化情報固有鍵、暗号化情報、鍵対応情報を読み出して別の記憶メディアに複製しても、この別の記憶メディアの独自の識別子から生成されるメディア秘密鍵では暗号化情報固有鍵を復号できず、従って情報の複製による不正利用を防止することができる。

【００１２】また、請求項２記載の本発明は、書換え不可能な独自の識別子を有する記憶メディアに記録された情報の利用を行う情報利用方法であって、前記記憶メディアの識別子を利用して、公開鍵方式のメディア公開鍵とメディア秘密鍵を生成し、不正利用を防止したい目的情報に対して生成された情報固有鍵を用いて目的情報を暗号化した暗号化情報と前記情報固有鍵を前記メディア公開鍵で暗号化した暗号化情報固有鍵を記録している前記記憶メディアから前記暗号化情報固有鍵を読み出し、この読み出した暗号化情報固有鍵を前記メディア秘密鍵で復号して、情報固有鍵を取り出し、前記暗号化情報を前記記憶メディアから読み出し、この暗号化情報を前記情報固有鍵で復号して前記目的情報を取り出して利用することを要旨とする。

【００１３】請求項２記載の本発明にあっては、記憶メディアから読み出した暗号化情報固有鍵を記憶メディアの識別子から生成したメディア秘密鍵で復号して、情報固有鍵を取り出し、情報固有鍵で暗号化情報を復号して目的情報を取り出すため、記憶メディアに記録されている暗号化情報固有鍵、暗号化情報、鍵対応情報を読み出して別の記憶メディアに複製しても、この別の記憶メデ

ィアの独自の識別子から生成されるメディア秘密鍵では暗号化情報固有鍵を復号できず、従って情報の複製による不正利用を防止することができる。

【００１４】更に、請求項３記載の本発明は、サーバにおいて不正利用を防止したい目的情報に対して生成された情報固有鍵を用いて目的情報を暗号化した暗号化情報と情報固有鍵をサーバ記憶装置に蓄積し、この蓄積されている暗号化情報と情報固有鍵を、情報記録装置に装着され、書換え不可能な独自の識別子を有する記憶メディアまで配送する情報配送方法であって、前記記憶メディアの識別子を利用して、公開鍵方式のメディア公開鍵とメディア秘密鍵を生成し、このメディア公開鍵をサーバに送信し、サーバにおいて前記メディア公開鍵で前記情報固有鍵を暗号化して暗号化情報固有鍵を生成し、前記暗号化情報固有鍵と前記暗号化情報を情報記録装置に送信し、情報記録装置は前記暗号化情報固有鍵と前記暗号化情報を受信して、記憶メディアに記録することを要旨とする。

【００１５】請求項３記載の本発明にあっては、情報記録装置からサーバに送信される記憶メディアの情報はメディア公開鍵のみであり、通信中に盗聴されても不正利用はできず、またサーバから情報記録装置に送信される情報は暗号化情報固有鍵と暗号化情報であり、暗号化情報固有鍵は記憶メディアの識別子から生成したメディア秘密鍵がなければ情報固有鍵に復号できず、この情報固有鍵がなければ暗号化情報から目的情報を復号できない。従って、暗号化情報固有鍵と暗号化情報は通信中に盗聴されても不正利用することはできない。

【００１６】請求項４記載の本発明は、情報提供側からの目的情報を情報利用側に配送し、書換え不可能な独自の識別子を有する記憶メディアに目的情報を記録し、この記録された目的情報を利用する情報の配送、記録および利用方法であって、情報提供側において、前記目的情報に対して情報固有鍵を生成し、この生成した情報固有鍵を用いて前記目的情報を暗号化した暗号化情報を生成し、この暗号化情報と前記情報固有鍵を記憶しておき、情報利用側において、前記記憶メディアの識別子を利用して、公開鍵方式のメディア公開鍵とメディア秘密鍵を生成し、このメディア公開鍵を情報提供側に配送し、情報提供側において、前記メディア公開鍵を受信し、このメディア公開鍵で前記情報固有鍵を暗号化した暗号化情報固有鍵を生成し、この生成した暗号化情報固有鍵と前記暗号化情報を情報利用側に配送し、情報利用側において、前記暗号化情報固有鍵と前記暗号化情報を受信し、この受信した暗号化情報固有鍵と暗号化情報を前記記憶メディアに記録し、情報利用側において、前記記憶メディアの識別子を利用して、公開鍵方式のメディア公開鍵とメディア秘密鍵を生成し、このメディア秘密鍵を用いて前記暗号化情報固有鍵を復号して情報固有鍵を取り出し、この情報固有鍵を用いて前記暗号化情報を復号して目的情報を取り出すことを要旨とする。

【００１７】請求項４記載の本発明にあっては、情報提供側において目的情報から生成される情報固有鍵を用いて目的情報を暗号化した暗号化情報を生成し、この暗号化情報と情報固有鍵を記憶しておき、情報利用側において記憶メディアの識別子を利用してメディア公開鍵とメディア秘密鍵を生成し、該メディア公開鍵を情報提供側に配送し、情報提供側において受信したメディア公開鍵で情報固有鍵を暗号化した暗号化情報固有鍵と暗号化情報を情報利用側に配送し、情報利用側において受信した暗号化情報固有鍵と暗号化情報を記憶メディアに記録し、情報利用側においてメディア秘密鍵を用いて暗号化情報固有鍵を復号して情報固有鍵を取り出し、この情報固有鍵を用いて暗号化情報を復号して目的情報を取り出すため、暗号化情報固有鍵、暗号化情報を記憶メディアから読み出して別の記憶メディアに複製しても、この別の記憶メディアの独自の識別子から生成されるメディア秘密鍵では暗号化情報固有鍵を復号できず、従って情報の複製による不正利用を防止することができるとともに、暗号化情報固有鍵は記憶メディアの識別子から生成したメディア秘密鍵がなければ情報固有鍵に復号できず、この情報固有鍵がなければ暗号化情報から目的情報を復号できないため、暗号化情報固有鍵と暗号化情報は通信中に盗聴されても不正利用することはできない。

【００１８】また、請求項５記載の本発明は、サーバにおいて不正利用を防止したい目的情報に対して生成された情報固有鍵を用いて目的情報を暗号化した暗号化情報が既に情報記録装置の記憶メディア内に記憶されており、サーバの記憶装置に蓄積されている情報固有鍵を、情報記録装置に装着され、書換え不可能な独自の識別子を有する記憶メディアまで配送する情報配送方法であって、前記記憶メディアの識別子を利用して、公開鍵方式のメディア公開鍵とメディア秘密鍵を生成し、このメディア公開鍵をサーバに送信し、サーバにおいて前記メディア公開鍵で前記情報固有鍵を暗号化して暗号化情報固有鍵を生成し、前記暗号化情報固有鍵を情報記録装置に送信し、情報記録装置は前記暗号化情報固有鍵を受信して、記憶メディアに記録することを要旨とする。

【００１９】請求項５記載の本発明にあっては、情報記録装置からサーバに送信される記憶メディアの情報はメディア公開鍵のみであり、通信中に盗聴されても不正利用はできず、またサーバから情報記録装置に送信される情報は暗号化情報固有鍵のみであり、暗号化情報固有鍵は記憶メディアの識別子から生成したメディア秘密鍵がなければ情報固有鍵に復号できず、従って暗号化情報固有鍵が通信中に盗聴されても不正利用することはできない。

【００２０】更に、請求項６記載の本発明は、書換え不可能な独自の識別子を有する記憶メディアを用いて情報の記録を行う情報記録方法であって、情報記録装置と情

報利用装置の間で共有され、利用者には秘密の利用共通鍵を用いて、前記記憶メディアの識別子を暗号化して第１の暗号情報Ｋ１を生成し、鍵サーバと情報記録装置の間で共有され、利用者には秘密の配送用共通鍵を用いて、前記第１の暗号情報Ｋ１を暗号化して第２の暗号情報Ｋ２を生成し、不正利用を防止したい目的情報に対して情報固有鍵を生成し、この情報固有鍵を用いて前記目的情報を暗号化した暗号化情報を生成し、前記情報固有鍵を前記第１の暗号情報Ｋ１で暗号化してＫ１暗号化情報固有鍵を生成し、前記暗号化情報と前記Ｋ１暗号化情報固有鍵を記憶メディアに記録することを要旨とする。

【００２１】請求項６記載の本発明にあっては、Ｋ１暗号化情報固有鍵から情報固有鍵を復号するには、第１の暗号情報Ｋ１が必要であり、この第１の暗号情報Ｋ１は記憶メディア独自の識別子から利用共通鍵を用いて生成されるため、記憶メディアから暗号化情報、Ｋ１暗号化情報固有鍵を別の記憶メディアに複製しても、別の記憶メディアの独自の識別子から生成される第１の暗号情報Ｋ１では復号できず、従って情報の複製による不正利用を防止することができる。

【００２２】請求項７記載の本発明は、書換え不可能な独自の識別子を有する記憶メディアに記録された情報の利用を行う情報利用方法であって、情報記録装置と情報利用装置の間で共有され、利用者には秘密の利用共通鍵を用いて、前記記憶メディアの識別子を暗号化して第１の暗号情報Ｋ１を生成し、前記情報固有鍵を前記第１の暗号情報Ｋ１で暗号化してＫ１暗号化情報固有鍵を生成し、不正利用を防止したい目的情報に対して生成された情報固有鍵を用いて目的情報を暗号化した暗号化情報と前記情報固有鍵を前記第１の暗号情報Ｋ１で暗号化したＫ１暗号化情報固有鍵が記録されている記憶メディアから前記Ｋ１暗号化情報固有鍵を読み出し、この読み出したＫ１暗号化情報固有鍵を前記第１の暗号情報Ｋ１で復号して、情報固有鍵を取り出し、前記暗号化情報を前記記憶メディアから読み出し、この暗号化情報を前記情報固有鍵で復号して前記目的情報を取り出して利用することを要旨とする。

【００２３】請求項７記載の本発明にあっては、記憶メディアから読み出したＫ１暗号化情報固有鍵を記憶メディアの識別子から生成した第１の暗号情報Ｋ１で復号して、情報固有鍵を取り出し、情報固有鍵で暗号化情報を復号して目的情報を取り出すため、記憶メディアに記録されているＫ１暗号化情報固有鍵、暗号化情報を読み出して別の記憶メディアに複製しても、別の記憶メディアの独自の識別子から生成される第１の暗号情報Ｋ１ではＫ１暗号化情報固有鍵を復号できず、従って情報の複製による不正利用を防止することができる。

【００２４】また、請求項８記載の本発明は、サーバにおいて不正利用を防止したい目的情報に対して生成された情報固有鍵を用いて目的情報を暗号化した暗号化情報と情報固有鍵をサーバ記憶装置に蓄積し、この蓄積されている暗号化情報と情報固有鍵を、情報記録装置に装着され、書換え不可能な独自の識別子を有する記憶メディアまで配送する情報配送方法であって、情報記録装置と情報利用装置の間で共有され、利用者には秘密の利用共通鍵を用いて、前記記憶メディアの識別子を暗号化して第１の暗号情報Ｋ１を生成し、サーバと情報記録装置の間で共有され、利用者には秘密の配送用共通鍵を用いて、前記第１の暗号情報Ｋ１を暗号化して第２の暗号情報Ｋ２を生成し、この第２の暗号情報Ｋ２をサーバに送信し、サーバにおいて前記第２の暗号情報Ｋ２を前記配送用共通鍵で復号して前記第１の暗号情報Ｋ１を生成し、この第１の暗号情報Ｋ１で前記情報固有鍵を暗号化してＫ１暗号化情報固有鍵を生成し、前記Ｋ１暗号化情報固有鍵と前記暗号化情報を情報記録装置に送信し、情報記録装置は前記Ｋ１暗号化情報固有鍵と前記暗号化情報を受信して、記憶メディアに記録することを要旨とする。

【００２５】請求項８記載の本発明にあっては、情報記録装置からサーバに送信される記憶メディアの情報は第２の暗号情報Ｋ２のみであり、第２の暗号情報Ｋ２が通信中に盗聴されても配送用共通鍵が知られない限り不正利用はできず、またサーバから情報記録装置に送信される情報はＫ１暗号化情報固有鍵と暗号化情報であり、Ｋ１暗号化情報固有鍵は利用サーバ鍵と記憶メディア独自の識別子がなければ情報固有鍵に復号できず、暗号化情報は情報固有鍵がなければ目的情報に復号できない。従って、Ｋ１暗号化情報固有鍵と暗号化情報は通信中に盗聴されても不正利用できない。

【００２６】更に、請求項９記載の本発明は、サーバにおいて不正利用を防止したい目的情報に対して生成された情報固有鍵を用いて目的情報を暗号化した暗号化情報が既に情報記録装置の記憶メディア内に記憶されており、サーバの記憶装置に蓄積されている情報固有鍵を、情報記録装置に装着され、書換え不可能な独自の識別子を有する記憶メディアまで配送する情報配送方法であって、前記記憶メディアの識別子を利用して、公開鍵方式のメディア公開鍵とメディア秘密鍵を生成し、このメディア公開鍵をサーバに送信し、情報記録装置と情報利用装置の間で共有され、利用者には秘密の利用共通鍵を用いて、前記記憶メディアの識別子を暗号化して第１の暗号情報Ｋ１を生成し、サーバと情報記録装置の間で共有され、利用者には秘密の配送用共通鍵を用いて、前記第１の暗号情報Ｋ１を暗号化して第２の暗号情報Ｋ２を生成し、この第２の暗号情報Ｋ２をサーバに送信し、サーバにおいて前記第２の暗号情報Ｋ２を前記配送用共通鍵で復号して前記第１の暗号情報Ｋ１を生成し、この第１の暗号情報Ｋ１で前記情報固有鍵を暗号化してＫ１暗号化情報固有鍵を生成し、前記Ｋ１暗号化情報固有鍵を情報記録装置に送信し、情報記録装置は前記Ｋ１暗号化情

報固有鍵を受信して、記憶メディアに記録することを要旨とする。

【００２７】請求項９記載の本発明にあっては、情報記録装置からサーバに送信される記憶メディアの情報は第２の暗号情報Ｋ２のみであり、この第２の暗号情報Ｋ２が通信中に盗聴されても配送用サーバ鍵が知られない限り不正利用はできず、またサーバから情報記録装置に送信される情報はＫ１暗号化情報固有鍵のみであり、Ｋ１暗号化情報固有鍵は利用サーバ鍵と記憶メディア独自の識別子がなければ情報固有鍵に復号できず、従ってＫ１暗号化情報固有鍵は通信中に盗聴されても不正利用できない。

【００２８】請求項１０記載の本発明は、書換え不可能な独自の識別子を有する記憶メディアを用いて情報の記録を行う情報記録方法であって、前記記憶メディアの識別子を利用して、公開鍵方式のメディア公開鍵とメディア秘密鍵を生成し、このメディア公開鍵を用いて暗号化した目的情報を記憶メディアに記録することを要旨とする。

【００２９】請求項１０記載の本発明にあっては、暗号化情報を復号するにはメディア秘密鍵が必要であり、メディア秘密鍵は記憶メディア独自の識別子から生成されるため、記憶メディアから暗号化情報が別の記憶メディアに複製されても、別の記憶メディア独自の識別子から生成されるメディア秘密鍵では暗号化情報を復号できず、従って情報の複製による不正利用を防止することができる。

【００３０】また、請求項１１記載の本発明は、書換え不可能な独自の識別子を有する記憶メディアに記録されている暗号化情報を利用する情報利用方法であって、前記記憶メディアの識別子を利用して、公開鍵方式のメディア公開鍵とメディア秘密鍵を生成し、前記記憶メディアに記録されている暗号化情報を読み出し、この暗号化情報を前記メディア秘密鍵で復号して、目的情報を取り出して利用することを要旨とする。

【００３１】請求項１１記載の本発明にあっては、記憶メディアから読み出した暗号化情報を記憶メディアの識別子から生成したメディア秘密鍵で復号して目的情報を取り出すため、記憶メディアに記録されている暗号化情報を読み出して別の記憶メディアに複製しても、別の記憶メディアの独自の識別子から生成されるメディア秘密鍵では暗号化情報を復号できず、従って情報の複製による不正利用を防止することができる。

【００３２】更に、請求項１２記載の本発明は、サーバに蓄積されている目的情報を、情報記録装置に装着され、書換え不可能な独自の識別子を有する記憶メディアまで配送する情報配送方法であって、前記記憶メディアの識別子を利用して、公開鍵方式のメディア公開鍵とメディア秘密鍵を生成し、このメディア公開鍵をサーバに送信し、サーバにおいて前記メディア公開鍵で前記目的情報を暗号化して暗号化情報を生成し、サーバは前記暗号化情報を情報記録装置に送信し、情報記録装置は前記暗号化情報を受信して、記憶メディアに記録することを要旨とする。

【００３３】請求項１２記載の本発明にあっては、情報記録装置からサーバに送信される情報はメディア公開鍵のみであり、メディア公開鍵は記憶メディア独自の識別子から生成されるものであるため、通信中に盗聴されても不正利用できない。また、サーバから情報記録装置に送信される目的情報はメディア公開鍵で暗号化されており、通信中に盗聴されても不正利用できない。

【００３４】

【発明の実施の形態】以下、図面を用いて本発明の実施の形態について説明する。図１は、本発明の第１の実施形態に係る記憶メディア識別子を利用した不正利用防止のための情報の記録、利用および配送方法を実施するシステム構成を示すブロック図である。図１に示す実施形態１のシステムは、記憶メディア１と、この記憶メディア１に情報を書き込む情報記録装置２と、記憶メディア１に格納された情報を利用する際に使う情報利用装置３と、情報を配信する鍵サーバ４から構成され、元の目的情報は情報提供者５から提供される。

【００３５】記憶メディア１は記憶メディア独自のＩＤ（識別子）１１と、通常の書換え可能な記憶領域１２から構成される。

【００３６】また記憶メディア１に情報を書き込む情報記録装置２は、公開鍵ペア生成処理部２１と情報記録処理部２２を持っており、記憶メディア１を装着した上で記憶メディア１からの記憶メディア独自のＩＤ１１の読み出しと、記憶領域１２への書き込みを行うことができる。

【００３７】情報を配信する鍵サーバ４は、メディア公開鍵を用いて情報固有鍵を暗号化した暗号化情報固有鍵を作成するための公開鍵暗号化処理部４１と、暗号化情報および情報固有鍵を蓄積する記憶装置４２と、情報暗号化処理部４３からなる。

【００３８】情報提供者５は予め目的情報Ｃを鍵サーバ４に送信し、鍵サーバ４内の情報暗号化処理部４３にて情報固有鍵Ｋｃとこの情報固有鍵Ｋｃで暗号化した暗号情報Ｅｃ（Ｋｃ，Ｃ）を作成しておき、情報固有鍵Ｋｃと暗号情報Ｅｃ（Ｋｃ，Ｃ）を鍵サーバ４内の記憶装置４２に記録しておく。

【００３９】目的情報を鍵サーバ４から記憶メディア１まで配送する場合には、まず、記憶メディア１から記憶メディア独自のＩＤ１１を読み出し、情報記録装置２内部の公開鍵ペア生成処理部２１で、記憶メディア独自のＩＤ１１を利用してメディア公開鍵Ｋｐｍとメディア秘密鍵Ｋｓｍを生成し、メディア公開鍵Ｋｐｍを鍵サーバ４に送信する。メディア公開鍵Ｋｐｍを受信した鍵サーバ４では、記憶装置４２から情報固有鍵Ｋｃを取り出

し、公開鍵暗号化処理部４１で、情報固有鍵Ｋｃをメディア公開鍵Ｋｐｍを用いて暗号化し、暗号化情報固有鍵Ｅｐ（Ｋｐｍ，Ｋｃ）を生成する。

【００４０】次いで、鍵サーバ４は暗号情報Ｅｃ（Ｋｃ，Ｃ）と暗号化情報固有鍵Ｅｐ（Ｋｐｍ，Ｋｃ）を情報記録装置２へ送信する。暗号情報Ｅｃ（Ｋｃ，Ｃ）と暗号化情報固有鍵Ｅｐ（Ｋｐｍ，Ｋｃ）を受け取った情報記録装置２では、情報記録処理部２２にて記憶メディア１の記憶領域１２へ暗号情報Ｅｃ（Ｋｃ，Ｃ）と暗号化情報固有鍵Ｅｐ（Ｋｐｍ，Ｋｃ）を記録する。

【００４１】この配送方法を利用して配送経路上の盗聴の脅威を考えた場合、配送経路上を流れるデータはメディア公開鍵Ｋｐｍと暗号情報Ｅｃ（Ｋｃ，Ｃ）と暗号化情報固有鍵Ｅｐ（Ｋｐｍ，Ｋｃ）であり、メディア秘密鍵Ｋｓｍがなければ暗号化情報固有鍵Ｅｐ（Ｋｐｍ，Ｋｃ）は復号できず、情報固有鍵Ｋｃがなければ暗号情報Ｅｃ（Ｋｃ，Ｃ）は復号できず、メディア公開鍵Ｋｐｍは盗聴されても問題がないために、配送経路上を流れるデータを盗聴されても目的情報Ｃを復元することができないため、安全である。

【００４２】次に、上記実施形態１で記憶メディア１に記録された情報を利用する方法について述べる。情報利用装置３は公開鍵ペア生成処理部３１と鍵復号処理部３２と情報復号処理部３３と情報利用処理部３４を持ち、記憶メディア１を装着した上で記憶メディア１からの記憶メディア独自のＩＤ１１の読み出しと、記憶領域１２からの読み出しを行うことができる。なお、公開鍵ペア生成処理部３１は情報記録装置２の公開鍵ペア生成処理部２１と同じアルゴリズムを用いて公開鍵および暗号鍵の生成を行うものとする。

【００４３】情報の配送後、情報を利用する場合、記憶メディア１は情報記録装置２から取り出され、情報利用装置３に装着されているものとする。

【００４４】情報を利用する際に、まず記憶メディア１から記憶メディア独自のＩＤ１１を読み出し、情報利用装置３内部の公開鍵ペア生成処理部３１で、記憶メディア独自のＩＤ１１を利用してメディア公開鍵Ｋｐｍとメディア秘密鍵Ｋｓｍを生成し、鍵復号処理部３２にメディア秘密鍵Ｋｓｍを渡し、鍵復号処理部３２は記憶メディア１の記憶領域１２から暗号化情報固有鍵Ｅｐ（Ｋｐｍ，Ｋｃ）を読み出し、暗号化情報固有鍵Ｅｐ（Ｋｐｍ，Ｋｃ）をメディア秘密鍵Ｋｓｍで復号し情報固有鍵Ｋｃを得て、情報復号処理部３３に渡し、情報復号処理部３３は記憶メディア１の記憶領域１２から暗号情報Ｅｃ（Ｋｃ，Ｃ）を読み出し、暗号情報Ｅｃ（Ｋｃ，Ｃ）を情報固有鍵Ｋｃで復号し目的情報Ｃを得て、情報利用処理部３４へ渡す。情報利用処理部３４は、目的情報Ｃを利用するための処理を行うものとし、ここではその処理を規定しないが、音楽、動画像、静止画像、テキスト等の各種情報の再生等が考えられる。

【００４５】ここで不正利用者が、記憶メディア１から暗号情報Ｅｃ（Ｋｃ，Ｃ）と暗号化情報固有鍵Ｅｐ（Ｋｐｍ，Ｋｃ）を読み出し、別の記憶メディアに複製した場合を考える。このとき、別の記憶メディアには記憶メディア独自のＩＤがあるが、これは書換えができないため複製することができない。複製した記憶メディアを用いて上記情報利用装置で情報を利用しようとした場合、公開鍵ペア生成処理部３１では、メディア公開鍵Ｋｐｍ′とメディア秘密鍵Ｋｓｍ′が生成されるが、このメディア秘密鍵Ｋｓｍ′では暗号化情報固有鍵Ｅｐ（Ｋｐｍ，Ｋｃ）から情報固有鍵Ｋｃを復号することはできない。このため、暗号情報Ｅｃ（ｋｃ，Ｃ）から目的情報Ｃを復号することもできず、結局複製した記憶メディアでは目的情報を利用することはできないため、情報は不正利用できない。一方、正当な利用者は記憶メディア１を、情報利用装置３の機能を備えた任意の装置に装着することで情報の利用が可能であり、可搬性を保つことができる。

【００４６】図２は、本発明の第２の実施形態に係る記憶メディア識別子を利用した不正利用防止のための情報の記録、利用および配送方法を実施するシステム構成を示すブロック図である。同図に示す実施形態２のシステムは、目的情報を情報固有鍵で暗号化した暗号化情報を情報提供者５においてＣＤ－ＲＯＭ等６やインターネット等の経路を通じて予め利用者に配送し、記憶メディア１の記憶領域１２に既に格納されている点が図１に示した実施形態１と異なるものである。

【００４７】すなわち、図２に示す実施形態２のシステムは、記憶メディア１と、記憶メディアに情報を書き込む情報記録装置２と、記憶メディア１に格納された情報を利用する際に使う情報利用装置３と、情報を配信する鍵サーバ４から構成され、元の目的情報は情報提供者５から提供される。

【００４８】記憶メディア１は記憶メディア独自のＩＤ１１と、通常の書換え可能な記憶領域１２から構成される。

【００４９】また、記憶メディア１に情報を書き込む情報記録装置２は、公開鍵ペア生成処理部２１と情報記録処理部２２を持っており、記憶メディア１を装着した上で記憶メディア１からの記憶メディア独自のＩＤ１１の読み出しと、記憶領域１２への書き込みを行うことができる。

【００５０】鍵情報を配信する鍵サーバ４は、メディア公開鍵を用いて情報固有鍵を暗号化した暗号化情報固有鍵を作成するための公開鍵暗号化処理部４１と、暗号化情報および情報固有鍵を蓄積する記憶装置４２と、情報暗号化処理部４３からなる。

【００５１】情報提供者は予め目的情報Ｃを鍵サーバ４に送信し、鍵サーバ４内の情報暗号化処理部４３にて情報固有鍵Ｋｃとこの情報固有鍵Ｋｃで目的情報を暗号化

した暗号情報Ｅｃ（Ｋｃ，Ｃ）を作成して、情報固有鍵Ｋｃを鍵サーバ４内の記憶装置４２に記録しておき、暗号情報Ｅｃ（Ｋｃ，Ｃ）は情報提供者がＣＤ－ＲＯＭやインターネット等の経路を通じて予め利用者まで情報を配送しており、暗号情報Ｅｃ（Ｋｃ，Ｃ）は既に記憶メディア１の記憶領域１２内に格納されているものとする。

【００５２】情報固有鍵Ｋｃを鍵サーバ４から記憶メディア１まで配送する場合には、まず、記憶メディア１から記憶メディア独自のＩＤ１１を読み出し、情報記録装置２内部の公開鍵ペア生成処理部２１で、メディア公開鍵Ｋｐｍとメディア秘密鍵Ｋｓｍを生成し、メディア公開鍵Ｋｐｍを鍵サーバ４に送信する。メディア公開鍵Ｋｐｍを受信した鍵サーバ４では、記憶装置４２から情報固有鍵Ｋｃを取り出し、公開鍵暗号化処理部４１で、情報固有鍵Ｋｃをメディア公開鍵Ｋｐｍを用いて暗号化し、暗号化情報固有鍵Ｅｐ（Ｋｐｍ，Ｋｃ）を生成する。

【００５３】次いで、鍵サーバ４は暗号化情報固有鍵Ｅｐ（Ｋｐｍ，Ｋｃ）を情報記録装置２へ送信する。暗号化情報固有鍵Ｅｐ（Ｋｐｍ，Ｋｃ）を受け取った情報記録装置２では、情報記録処理部２２にて記憶メディア１の記憶領域１２へ、暗号化情報固有鍵Ｅｐ（Ｋｐｍ，Ｋｃ）を記録する。この配送方法において配送経路上の盗聴の脅威を考えた場合、配送経路上を流れるデータはメディア公開鍵Ｋｐｍと暗号化情報固有鍵Ｅｐ（Ｋｐｍ，Ｋｃ）であり、メディア秘密鍵Ｋｓｍがなければ暗号化情報固有鍵Ｅｐ（Ｋｐｍ，Ｋｃ）は復号できず、例え盗聴者が暗号情報Ｅｃ（Ｋｃ，Ｃ）を入手していたとしても情報固有鍵Ｋｃがなければ暗号情報Ｅｃ（Ｋｃ，Ｃ）は復号できず、メディア公開鍵Ｋｐｍは盗聴されても問題がないために、配送経路上を流れるデータを盗聴されても目的情報Ｃを復元することができないため、安全である。

【００５４】また、実施形態２の方法で記憶メディア１に記録された情報を利用する場合の方法については、実施形態１の情報利用方法と同じであるため、省略する。実施形態２の場合、目的情報Ｃが大容量の場合でも鍵サーバ４と情報記録装置２の間の通信量は大きくならないため利用者の負担を減らすことができる。

【００５５】図３は、本発明の第３の実施形態に係る記憶メディア識別子を利用した不正利用防止のための情報の記録、利用および配送方法を実施するシステム構成を示すブロック図である。同図に示す実施形態３のシステムは、記憶メディア１と、記憶メディアに情報を書き込む情報記録装置７と、記憶メディア１に格納された情報を利用する際に使う情報利用装置８と、情報を配信する鍵サーバ９から構成され、元の目的情報は情報提供者５から提供される。

【００５６】記憶メディア１は記憶メディア独自のＩＤ１１と、通常の書換え可能な記憶領域１２から構成される。

【００５７】また、記憶メディア１に情報を書き込む情報記録装置７は、Ｋ１生成処理部７１とＫ２生成処理部７２と情報記録処理部７３を持っており、記憶メディア１を装着した上で記憶メディア１からの記憶メディア独自のＩＤ１１の読み出しと、記憶領域１２への書き込みを行うことができる。

【００５８】情報を配信する鍵サーバ９は、配送用共通鍵を用いてＫ２からＫ１を復号するＫ２復号化処理部９１と、Ｋ１を用いて情報固有鍵を暗号化したＫ１暗号化情報固有鍵を作成するための鍵暗号化処理部９２と、暗号化情報および情報固有鍵を蓄積する記憶装置９３と、情報暗号化処理部９４からなる。

【００５９】情報提供者は予め目的情報Ｃを鍵サーバ９に送信し、鍵サーバ９内の情報暗号化処理部９４にて情報固有鍵Ｋｃと暗号情報Ｅｃ（Ｋｃ，Ｃ）を作成しておき、情報固有鍵Ｋｃと暗号情報Ｅｃ（Ｋｃ，Ｃ）は鍵サーバ９内の記憶装置９３に記録しておく。

【００６０】目的情報を鍵サーバ９から記憶メディア１まで配送する場合には、まず、記憶メディア１から記憶メディア独自のＩＤ１１を読み出し、この記憶メディア独自のＩＤ１１から情報記録装置７内部のＫ１生成処理部７１で利用共通鍵を用いてＫ１を生成し、次のそのＫ１から情報記録装置７内部のＫ２生成処理部７２で配送用共通鍵を用いてＫ２を生成し、Ｋ２を鍵サーバ９に送信する。Ｋ２を受信した鍵サーバ９では、まずＫ２復号化処理部で配送用共通鍵を用いてＫ２からＫ１を復号し、記憶装置９３から情報固有鍵Ｋｃを取り出し、鍵暗号化処理部９２で、情報固有鍵ＫｃをＫ１を用いて暗号化し、Ｋ１暗号化情報固有鍵Ｅｃ（Ｋ１，Ｋｃ）を生成する。

【００６１】次いで、鍵サーバ９は暗号情報Ｅｃ（Ｋｃ，Ｃ）とＫ１暗号化情報固有鍵Ｅｃ（Ｋ１，Ｋｃ）を情報記録装置７へ送信する。暗号情報Ｅｃ（Ｋｃ，Ｃ）とＫ１暗号化情報固有鍵Ｅｃ（Ｋ１，Ｋｃ）を受け取った情報記録装置７では、情報記録処理部７３にて記憶メディア１の記憶領域１２へ、暗号情報Ｅｃ（Ｋｃ，Ｃ）とＫ１暗号化情報固有鍵Ｅｃ（Ｋ１，Ｋｃ）を記録する。

【００６２】この配送方法を利用して配送経路上の盗聴の脅威を考えた場合、配送経路上を流れるデータはＫ２と暗号情報Ｅｃ（Ｋｃ，Ｃ）とＫ１暗号化情報固有鍵Ｅｃ（Ｋ１，Ｋｃ）であり、配送用共通鍵を知らなければＫ２からＫ１を求めることはできず、Ｋ１がなければＫ１暗号化情報固有鍵Ｅｃ（Ｋ１，Ｋｃ）から情報固有鍵Ｋｃは復号できず、情報固有鍵Ｋｃがなければ暗号情報Ｅｃ（Ｋｃ，Ｃ）は復号できないため、配送経路上を流れるデータを盗聴されても目的情報Ｃを復元することができないため、安全である。

【００６３】次に、上記実施形態３で記憶メディア１に記録された情報を利用する方法について述べる。情報利用装置８はＫ１生成処理部８１と鍵復号処理部８２と情報復号処理部８３と情報利用処理部８４を持ち、記憶メディア１を装着した上で記憶メディア１からの記憶メディア独自のＩＤ１１の読み出しと、記憶領域１２からの読み出しを行うことができる。なお、Ｋ１生成処理部８１は情報記録装置７のＫ１生成処理部７１と同じアルゴリズムを用い、またＫ１生成の際に用いる利用共通鍵を情報記録装置７のＫ１生成処理部７１と共有しているものとする。

【００６４】情報の配送後、情報を利用する場合、記憶メディア１は情報記録装置７から取り出し、情報利用装置８に装着されているものとする。

【００６５】情報を利用する際に、まず記憶メディア１から記憶メディア独自のＩＤ１１を読み出し、この記憶メディア独自のＩＤ１１から情報利用装置８内部のＫ１生成処理部８１で利用共通鍵を用いてＫ１を生成し、鍵復号処理部８２にＫ１を渡し、鍵復号処理部８２は記憶メディア１の記憶領域１２からＫ１暗号化情報固有鍵Ｅｃ（Ｋ１，Ｋｃ）を読み出し、Ｋ１暗号化情報固有鍵Ｅｃ（Ｋ１，Ｋｃ）をＫ１で復号し情報固有鍵Ｋｃを得て、情報復号処理部８３に渡し、情報復号処理部８３は記憶メディア１の記憶領域１２から暗号情報Ｅｃ（Ｋｃ，Ｃ）を読み出し、暗号情報Ｅｃ（Ｋｃ，Ｃ）を情報固有鍵Ｋｃで復号し目的情報Ｃを得て、情報利用処理部８４を渡す。情報利用処理部８４は、目的情報Ｃを利用するための処理を行うものとし、ここではその処理を規定しないが、音楽、動画像、静止画像、テキスト等の各種情報の再生などが考えられる。

【００６６】ここで不正利用者が、記憶メディア１から暗号情報Ｅｃ（Ｋｃ，Ｃ）とＫ１暗号化情報固有鍵Ｅｃ（Ｋ１，Ｋｃ）を読み出し、別の記憶メディアに複製した場合を考える。このとき、別の記憶メディアには記憶メディア独自のＩＤがあるが、これは書換えができないため複製することができない。複製した記憶メディアを用いて上記情報利用装置で情報を利用しようとした場合、Ｋ１生成処理部３１では、Ｋ１′が生成されるが、このＫ１′ではＫ１暗号化情報固有鍵Ｅｃ（Ｋ１，Ｋｃ）から情報固有鍵Ｋｃを復号することはできない。このため、暗号情報Ｅｃ（Ｋｃ，Ｃ）から目的情報Ｃを復号することもできず、結局複製した記憶メディアでは目的情報を利用することはできないため、情報は不正利用できない。一方、正当な利用者は記憶メディア１を、情報利用装置３の機能を備えた任意の装置に装着することで情報の利用が可能であり、可搬性を保つことができる。

【００６７】図４は、本発明の第４の実施形態に係る記憶メディア識別子を利用した不正利用防止のための情報の記録、利用および配送方法を実施するシステム構成を示すブロック図である。同図に示す実施形態４のシステムは、目的情報を情報固有鍵で暗号化した暗号化情報を情報提供者５においてＣＤ－ＲＯＭ等６やインターネット等の経路を通じて予め利用者に配送し、記憶メディア１の記憶領域１２に既に格納されている点が図３に示した実施形態３と異なるものである。

【００６８】すなわち、図４に示す実施形態４のシステムは、記憶メディア１と、記憶メディアに情報を書き込む情報記録装置７と、記憶メディア１に格納された情報を利用する際に使う情報利用装置８と、情報を配信する鍵サーバ９から構成され、元の目的情報は情報提供者５から提供される。

【００６９】記憶メディア１は記憶メディア独自のＩＤ１１と、通常の書換え可能な記憶領域１２から構成される。

【００７０】また、記憶メディア１に情報を書き込む情報記録装置７は、Ｋ１生成処理部７１とＫ２生成処理部７２と情報記録処理部７３を持っており、記憶メディア１を装着した上で記憶メディア１からの記憶メディア独自のＩＤ１１の読み出しと、記憶領域１２への書き込みを行うことができる。

【００７１】情報を配信する鍵サーバ９は、配送用共通鍵を用いてＫ２からＫ１を復号するＫ２復号化処理部９１と、Ｋ１を用いて情報固有鍵を暗号化したＫ１暗号化情報固有鍵を作成するための鍵暗号化処理部９２と、暗号化情報および情報固有鍵を蓄積する記憶装置９３と、情報暗号化処理部９４からなる。

【００７２】情報提供者は予め目的情報Ｃを鍵サーバ９に送信し、鍵サーバ９内の情報暗号化処理部９４にて情報固有鍵Ｋｃとこの情報固有鍵Ｋｃで目的情報Ｃを暗号化した暗号情報Ｅｃ（Ｋｃ，Ｃ）を作成し、情報固有鍵Ｋｃは鍵サーバ９内の記憶装置９３に記録しておき、暗号情報Ｅｃ（Ｋｃ，Ｃ）は情報提供者がＣＤ－ＲＯＭやインターネット等の経路を通じて予め利用者まで情報を配送しており、暗号情報Ｅｃ（Ｋｃ，Ｃ）は既に記憶メディア１の記憶領域１２内に格納されているものとする。

【００７３】情報固有鍵Ｋｃを鍵サーバ９から記憶メディア１まで配送する場合には、まず、記憶メディア１から記憶メディア独自のＩＤ１１を読み出し、情報記録装置７内部のＫ１生成処理部７１で利用共通鍵を用いてＫ１を生成し、次にそのＫ１から情報記録装置７内部のＫ２生成処理部７２で配送用共通鍵を用いてＫ２を生成し、Ｋ２を鍵サーバ９に送信する。Ｋ２を受信した鍵サーバ９では、まずＫ２復号化処理部で配送用共通鍵を用いてＫ２からＫ１を復号し、記憶装置９３から情報固有鍵Ｋｃを取り出し、鍵暗号化処理部９２で、情報固有鍵ＫｃをＫ１を用いて暗号化し、Ｋ１暗号化情報固有鍵Ｅｃ（Ｋ１，Ｋｃ）を生成する。

【００７４】次いで、鍵サーバ９はＫ１暗号化情報固有

鍵Ｅｃ（Ｋ１，Ｋｃ）を情報記録装置７へ送信する。Ｋ１暗号化情報固有鍵Ｅｃ（Ｋ１，Ｋｃ）を受け取った情報記録装置７では、情報記録処理部７３にて記憶メディア１の記憶領域１２に暗号情報Ｅｃ（Ｋｃ，Ｃ）とＫ１暗号化情報固有鍵Ｅｃ（Ｋ１，Ｋｃ）を記録する。

【００７５】この配送方法において、配送経路上の盗聴の脅威を考えた場合、配送経路上を流れるデータはＫ２とＫ１暗号化情報固有鍵Ｅｃ（Ｋ１，Ｋｃ）であり、配送用共通鍵を知らなければＫ２からＫ１を求めることはできず、Ｋ１がなければＫ１暗号化情報固有鍵Ｅｃ（Ｋ１，Ｋｃ）から情報固有鍵Ｋｃは復号できず、情報固有鍵Ｋｃがなければ暗号情報Ｅｃ（Ｋｃ，Ｃ）は復号できないため配送経路上を流れるデータを盗聴されても目的情報Ｃを復元することができないため、安全である。

【００７６】また、実施形態４の方法で記憶メディア１に記録された情報を利用する場合の方法については、実施形態３の情報利用方法と同じであるため、省略する。実施形態４の場合、目的情報Ｃが大容量の場合でも鍵サーバ９と情報記録装置７の間の通信量は大きくならないため利用者の負担を減らすことができる。

【００７７】図５は、本発明の第５の実施形態に係る記憶メディア識別子を利用した不正利用防止のための情報の記録、利用および配送方法を実施するシステム構成を示すブロック図である。同図に示す実施形態５のシステムは、情報固有鍵の利用を省略しつつも書換え不可能なメディアＩＤを利用することにより複製による不正使用の防止、可搬性の維持、盗聴に対する防御を達成するものである。このシステムは、記憶メディア１と、この記憶メディア１に情報を書き込む情報記録装置２と、記憶メディア１に格納された情報を利用する際に使う情報利用装置３と、情報を配信する鍵サーバ１０とから構成され、元の目的情報は情報提供者５から提供される。

【００７８】記憶メディア１は、記憶メディア独自のＩＤ１１と、通常の書換え可能な記憶領域１２から構成されている。

【００７９】また、記憶メディア１に情報を書き込む情報記録装置２は、公開鍵ペア生成処理部２１と情報記録処理部２２を有し、記憶メディア１を装着した上で記憶メディア１からの記憶メディア独自のＩＤ１１の読み出しと、記憶領域１２への書き込みを行うことができる。

【００８０】情報を配信する鍵サーバ１０は、情報提供者５からの目的情報を記憶する記憶装置１０１と、この記憶装置１０１に記憶されている目的情報をメディア公開鍵を用いて暗号化する情報暗号化処理部１０２を有する。情報提供者５からの目的情報は、予め鍵サーバ１０に送信され、鍵サーバ１０の記憶装置１０１に記録されている。

【００８１】目的情報を鍵サーバ１０から記憶メディア１まで配送する場合には、まず記憶メディア１から記憶メディア独自のＩＤ１１を読み出し、情報記録装置２内の公開鍵ペア生成処理部２１で記憶メディア独自のＩＤ１１を利用して、メディア公開鍵Ｋｐｍとメディア秘密鍵Ｋｓｍを生成し、メディア公開鍵Ｋｐｍを鍵サーバ１０に送信する。メディア公開鍵Ｋｐｍを受信した鍵サーバ１０は、記憶装置１０１から目的情報を読み出し、情報暗号化処理部１０２において目的情報をメディア公開鍵Ｋｐｍで暗号化し、暗号情報Ｅｃ（Ｋｐｍ，Ｃ）を生成する。

【００８２】それから、鍵サーバ１０は、暗号情報Ｅｃ（Ｋｐｍ，Ｃ）を情報記録装置２に送信する。情報記録装置２は、暗号情報Ｅｃ（Ｋｐｍ，Ｃ）を受信すると、情報記録処理部２２にて記憶メディア１の記憶領域１２に暗号情報Ｅｃ（Ｋｐｍ，Ｃ）を記録する。

【００８３】この配送方法を利用した配送経路上の盗聴の脅威を考えた場合、配送経路上のデータはメディア公開鍵Ｋｐｍと暗号情報Ｅｃ（Ｋｐｍ，Ｃ）であり、メディア秘密鍵Ｋｓｍがなければ暗号情報Ｅｃ（Ｋｐｍ，Ｃ）を復号できないため、メディア公開鍵Ｋｐｍが盗聴されても問題がない。従って、配送経路上を流れるデータを盗聴されても目的情報Ｃを復元することはできず、安全である。

【００８４】次に、実施形態５において記憶メディア１に記録された情報を利用する方法について説明する。情報利用装置３は、公開鍵ペア生成処理部３１、情報復号処理部３３、および情報利用処理部３４を有し、記憶メディア１を装着した上で記憶メディア１からの記憶メディア独自のＩＤ１１の読み出しと、記憶領域１２からの読み出しを行うことができる。なお、公開鍵ペア生成処理部３１は情報記録装置２の公開鍵ペア生成処理部２１と同じアルゴリズムを用いて、公開鍵および暗号鍵の生成を行うものである。

【００８５】情報の配送後、情報を利用する場合、記憶メディア１は情報記録装置２から取り出され、情報利用装置３に装着されているものとする。

【００８６】情報を利用する際には、まず記憶メディア１から記憶メディア独自のＩＤ１１を読み出し、情報利用装置３内の公開鍵ペア生成処理部３１で記憶メディア独自のＩＤ１１を利用して、メディア公開鍵Ｋｐｍとメディア秘密鍵Ｋｓｍを生成し、情報復号処理部３３にメディア秘密鍵Ｋｓｍを渡す。鍵復号処理部３２は、記憶メディア１の記憶領域１２から暗号情報Ｅｃ（Ｋｐｍ，Ｃ）を読み出し、この暗号情報Ｅｃ（Ｋｐｍ，Ｃ）をメディア秘密鍵Ｋｓｍで復号して、目的情報Ｃを得て、情報利用処理部３４に渡す。情報利用処理部３４は、目的情報Ｃを利用するための処理を行うものであり、ここではその処理は規定しないが、例えば音楽、動画像、静止画像、テキスト等の各種情報の再生等が考えられる。

【００８７】ここで不正利用者が記憶メディア１から暗号信号Ｅｃ（Ｋｐｍ，Ｃ）を読み出し、別の記憶メディア１に複製する場合を考える。この時、別の記憶メディ

アには記憶メディア独自のＩＤがあるが、これは書換えができないため複製することはできない。複製した記憶メディアを用いて、情報利用装置で情報を利用しようとした場合、公開鍵ペア生成処理部３１ではメディア公開鍵Ｋｐｍ′とメディア秘密鍵Ｋｓｍ′が生成されるが、このメディア秘密鍵Ｋｓｍ′では暗号情報Ｅｃ（Ｋｐｍ，Ｃ）を復号することはできない。このため、暗号情報Ｅｃ（Ｋｐｍ，Ｃ）から目的情報Ｃを復号することもできず、結局複製した記憶メディアでは目的情報を利用することはできないため、情報を不正利用することはできない。

【００８８】

【発明の効果】以上説明したように、本発明によれば、記憶メディアに記録された情報を複製されても、記憶メディア独自の識別子は複製できないので、複製した暗号化情報固有鍵から情報固有鍵を復号することはできず、従って暗号化情報から目的情報を復号することができず、不正に複製を取っても目的情報の不正利用はできない。

【００８９】また、本発明によれば、通信中の情報が盗聴された場合でも、メディア公開鍵、暗号化情報固有鍵、暗号化情報から目的情報を復号することができず、安全に情報を配送することができる。

【００９０】更に、本発明によれば、目的情報は記憶メディアに記憶され持ち運びが容易にできるので、目的情報の可搬性を上げることができる。

【００９１】本発明によれば、一般に公開鍵暗号方式の復号処理よりも共通鍵暗号の復号処理の方が処理量が少なく、暗号化情報よりも暗号化情報固有鍵が十分小さい場合に、暗号化情報の復号に公開鍵暗号方式を用いる手法よりも処理量を減らすことができる。

【００９２】また、本発明によれば、情報固有鍵を用いずにメディア公開鍵で暗号化された暗号化情報を復号するにはメディア秘密鍵が必要であり、メディア秘密鍵は記憶メディア独自の識別子から生成されるので、記憶メディアから暗号化情報が別の記憶メディアに複製されても、別の記憶メディア独自の識別子から生成されるメディア秘密鍵では暗号化情報を復号できず、従って情報の複製による不正利用を防止することができる。

【００９３】更に、本発明によれば、情報記録装置からサーバに送信される情報はメディア公開鍵のみであり、メディア公開鍵は記憶メディア独自の識別子から生成されるものであるので、通信中に盗聴されても不正利用できない。また、サーバから情報記録装置に送信される目的情報はメディア公開鍵で暗号化されており、メディア秘密鍵は記憶メディア独自の識別子から生成されるので、通信中に盗聴されても不正利用できない。

【図面の簡単な説明】

【図１】本発明の第１の実施形態に係る記憶メディア識別子を利用した不正利用防止のための情報の記録、利用および配送方法を実施するシステム構成を示すブロック図である。

【図２】本発明の第２の実施形態に係る記憶メディア識別子を利用した不正利用防止のための情報の記録、利用および配送方法を実施するシステム構成を示すブロック図である。

【図３】本発明の第３の実施形態に係る記憶メディア識別子を利用した不正利用防止のための情報の記録、利用および配送方法を実施するシステム構成を示すブロック図である。

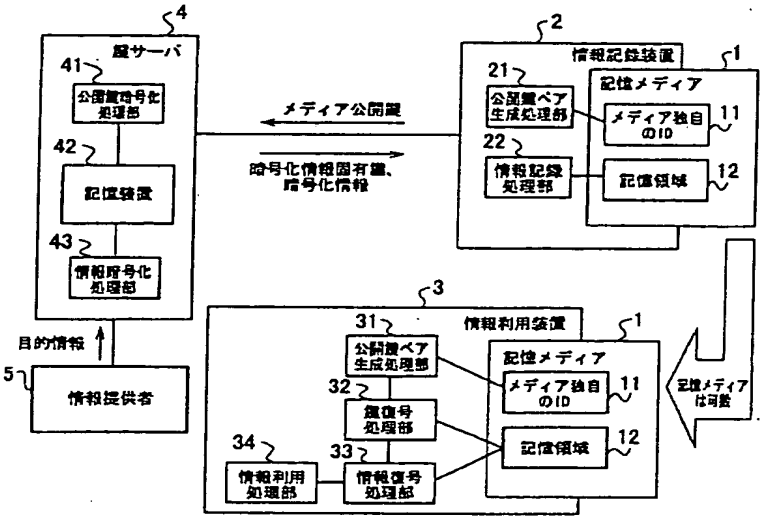
【図４】本発明の第４の実施形態に係る記憶メディア識別子を利用した不正利用防止のための情報の記録、利用および配送方法を実施するシステム構成を示すブロック図である。

【図５】本発明の第５の実施形態に係る記憶メディア識別子を利用した不正利用防止のための情報の記録、利用および配送方法を実施するシステム構成を示すブロック図である。

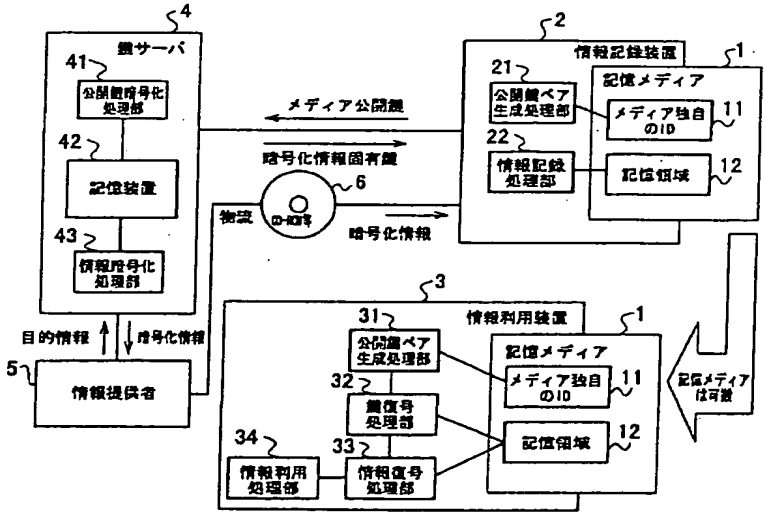
【符号の説明】

１　記憶メディア
２　情報記録装置
３　情報利用装置
４　鍵サーバ
１１　記憶メディア独自のＩＤ
１２　記憶領域
２１，３１　公開鍵ペア生成処理部
２２　情報記録処理部
３２　鍵復号処理部
３３　情報復号処理部
３４　情報利用処理部
４１　公開鍵暗号化処理部
４２　記憶装置
４３　情報暗号化処理部

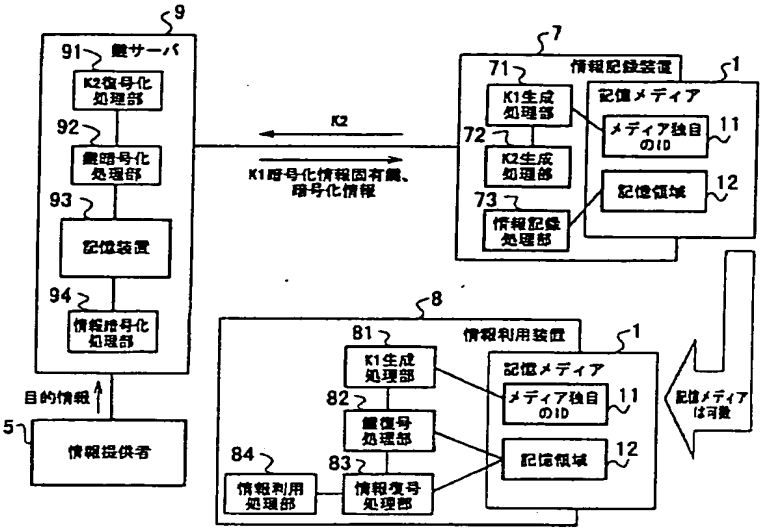
【図１】


4
鍵サーバ
41
公開鍵暗号化処理部
42
記憶装置
43
情報暗号化処理部
目的情報
5
情報提供者
メディア公開鍵
暗号化情報固有鍵、暗号化情報
2
情報記録装置
1
記憶メディア
21
公開鍵ペア生成処理部
メディア独自のID
11
22
情報記録処理部
記憶領域
12
3
情報利用装置
31
公開鍵ペア生成処理部
32
鍵復号処理部
34
情報利用処理部
33
情報復号処理部
記憶メディアは可搬

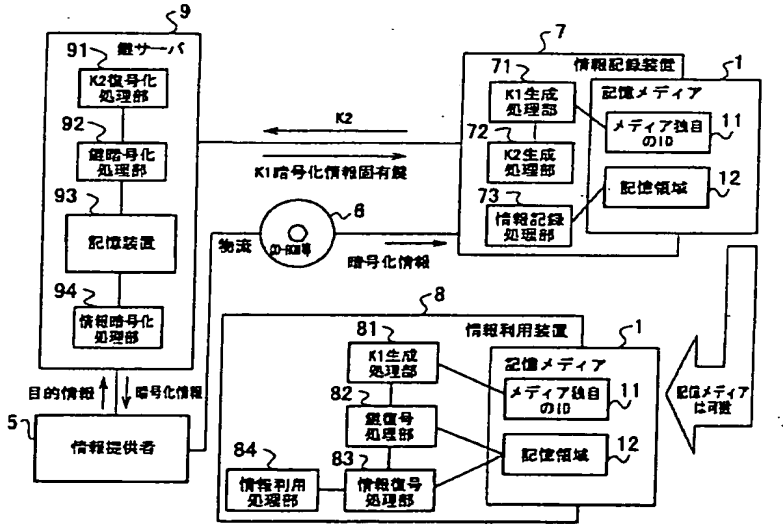
【図２】


4
鍵サーバ
41
公開鍵暗号化処理部
42
記憶装置
43
情報暗号化処理部
目的情報
暗号化情報
5
情報提供者
メディア公開鍵
暗号化情報固有鍵
6
物流
暗号化情報
2
情報記録装置
1
記憶メディア
21
公開鍵ペア生成処理部
メディア独自のID
11
22
情報記録処理部
記憶領域
12
3
情報利用装置
31
公開鍵ペア生成処理部
32
鍵復号処理部
34
情報利用処理部
33
情報復号処理部
記憶メディアは可搬

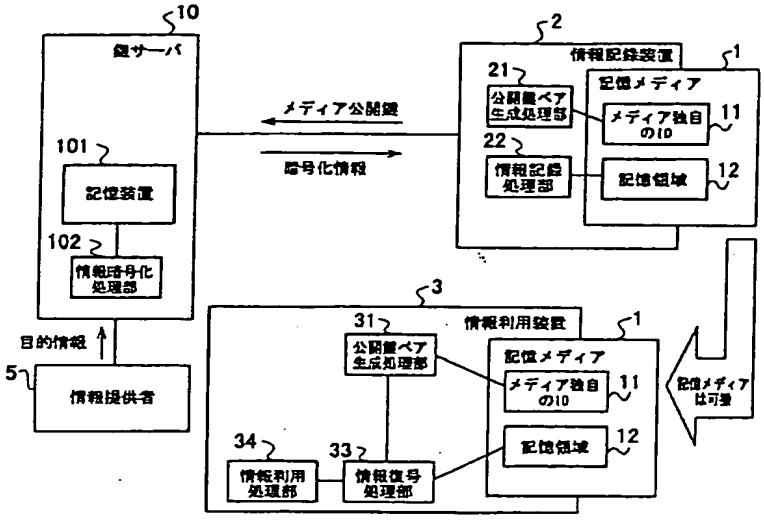
【図３】


9
91
鍵サーバ
K2復号化処理部
92
鍵暗号化処理部
93
記憶装置
94
情報暗号化処理部
目的情報
5
情報提供者
K2
K1暗号化情報固有鍵、暗号化情報
7
71
情報記録装置
K1生成処理部
72
K2生成処理部
73
情報記録処理部
1
記憶メディア
メディア独自のID
11
記憶領域
12
8
81
情報利用装置
K1生成処理部
82
鍵復号処理部
83
情報復号処理部
84
情報利用処理部
記憶メディアは可搬

【図４】


9
91
鍵サーバ
K2復号化処理部
92
鍵暗号化処理部
93
記憶装置
94
情報暗号化処理部
目的情報
暗号化情報
5
情報提供者
K2
K1暗号化情報固有鍵
6
物流
ID-読取
暗号化情報
7
71
情報記録装置
K1生成処理部
72
K2生成処理部
73
情報記録処理部
1
記憶メディア
メディア独自のID
11
記憶領域
12
8
81
情報利用装置
K1生成処理部
82
鍵復号処理部
83
情報復号処理部
84
情報利用処理部
記憶メディアは可搬

【図５】



フロントページの続き

(72)発明者　三宅　延久
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内
(72)発明者　庵　祥子
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内
(72)発明者　有田　一穂
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内

Ｆターム(参考)　5B017 AA06 AA07 BA05 BA07 BB02
BB07 CA09 CA15 CA16
5J104 AA12 AA16 EA16 EA17 EA22
EA26 NA02 NA36 NA37 PA07
PA14
9A001 EE03